ment abdicates its responsibility—as it largely has in the US to date—we end up with an insecure Internet+ that only serves short-term commercial and military interests.

Despite the pessimistic tone of much of this book, I am optimistic about cybersecurity in the long term. Eventually, we will solve this.

Otto von Bismarck observed: "Politics is the art of the possible." To that I reply: Technology is the science of the possible. But politics and technology offer different possibilities, and to understand this is to realize that politicians and technologists define "possible" very differently. As a technologist, I want to arrive at the correct answer or the best solution to a problem. A politician, on the other hand, is pragmatic, looking not for what's right or what's best, but for what he or she can actually accomplish.

Today, technology and policy are inextricably intertwined. The scenarios I've outlined—both the technological and economic trends causing them and the political changes needed to fix them—come from my years of involvement in the development of Internet security technology and policy. An understanding of both is critical.

Over the past couple of decades, we've seen many misguided recommendations for Internet security policy. Examples include the FBI's insistence that computer devices be designed to facilitate government access in order to repel the bugbear of "going dark," the vulnerability equities process by which government agencies determine whether to disclose and fix vulnerabilities or use them to attack other systems, the failure of paperless touch-screen voting machines to produce trustworthy elections, and the DMCA. If you followed any of these policy debates as they unfolded, you heard policy makers and technologists talking past each other.

You saw this in Chapters 6, 7, 8, and 9—a bunch of great ideas that won't happen anytime soon. You saw the counterpart to this in Chapter 11—what tech-impaired policy makers might do to make things worse.

The Internet+ will exacerbate most, if not all, of these problems. The growing divide between Washington and Silicon Valley—the mutual mistrust between governments and tech companies—is dangerous. As computer security issues pervade other industries, we'll see similar disconnects between technology and policy—and between technologists and policy makers. British solicitor Nick Bohm eloquently phrased it as "the lawyers and engineers whose arguments pass through one other like angry ghosts."

This division isn't new. Addressing the 2014 Munich Security Conference, Estonian president Toomas Hendrik Ilves observed:

> I think much of the problem we face today represents the culmination of a problem diagnosed 55 years ago by C. P. Snow in his essay "The Two Cultures": the absence of dialogue between the scientific-technological and the humanist traditions. When Snow wrote his classic essay, he bemoaned that neither culture understood or impinged on the other. Today, bereft of understanding of fundamental issues and writings in the development of liberal democracy, computer geeks devise ever better ways to track people . . . simply because they can and it's cool. Humanists on the other hand do not understand the underlying technology and are convinced, for example, that tracking meta-data means the government reads their emails.
>
> C. P. Snow's two cultures not only do not talk to each other, they simply act as if the other doesn't exist.

That might have been acceptable in 1959, because technology and policy didn't interact with each other often or as closely as they do now. Today, it's a different story. Technological mishaps can have catastrophic consequences. It's time we crossed the streams. Policy makers and technologists need to work together. They need to learn each other's languages and educate each other.

The solution to this consists of two halves. First, policy makers need to understand technology. In my fantasy world, policy decisions look like they do in *Star Trek: The Next Generation*. There, everyone sits around a conference table, and the technologists explain the meaning of data and scientific realities to Captain Picard. Picard listens, considers the facts and his options, then makes a policy decision informed by science and technology.

That's not the way it works in the real world. Too often, policy makers don't understand science and technology. Too often, they have their agendas and preconceived notions, and they try to force the science to fit. Sometimes they even brag about not understanding technologies. Lobbyists are often happy to provide pseudoscience to match any policies. And their

plates are so full with a range of obligations that they don't have the time to fully comprehend the information that's put in front of them.

In Chapter 11, I mentioned Australia's attempts to legislate backdoors in security systems. Answering a press question in 2017, Prime Minister Malcolm Turnbull said: "Well the laws of Australia prevail in Australia, I can assure you of that. The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia." This statement, of course, is laughably wrong and attracted widespread, justified mockery. When the laws of Australia and mathematics contradict, the laws of mathematics will prevail every time.

Similarly, I don't think most policy makers fully comprehend the risks posed by large corporate-held databases full of our personal information, or the threats to our nation's critical infrastructure from both hackers and nation-states. I don't think they understand the fundamental concepts of computer security that I enumerated in Chapter 1, or the failures I discussed in Chapters 2 and 3.

Policy must take mathematics, science, and engineering into account. Policy shouldn't pretend that things that are true are not. Policy can't force things to be true that are not. I regard policy as the primary mechanism for addressing our computer security problems. All of our security policy issues will have strong technological components, but we will never get the policy right if policy makers get the technology wrong. This isn't about turning policy makers into technologists, but ensuring that they have a technological intuition that helps them understand technologists and make decisions about technology. Ignorance is no longer an option.

That said, as important as it will be for policy makers to understand technology, that won't be enough. The second half of solving the divide between tech and policy is for technologists to get involved in policy. Not all of them, of course, but we need more public-interest technologists like these people:

Latanya Sweeney directs the Data Privacy Lab at Harvard, where she's a professor of government and technology. She's probably the best analyst of de-anonymization, and regularly demonstrates how different anonymity techniques don't work. She has also exposed bias in Internet algorithms, and has made significant contributions to privacy technologies. In 2014, she spent a year as chief technologist for the Federal Trade Commission.

Susan Landau is currently a professor in cybersecurity at Tufts University. She's a cryptographer and computer security technologist who has worked at both Sun Microsystems and Google. Today, she's easily the best thinker and communicator we have on the value of ubiquitous encryption in the face of the FBI's "going dark" fears, writing books and articles, and testifying before Congress on the topic.

Ed Felten is a Princeton computer science professor who has done considerable security research in a variety of areas. He's probably best known for his analysis of the security of electronic voting machines. In 2010, he was appointed chief technologist for the Federal Trade Commission, and he was deputy US chief technology officer from 2015 to 2017.

I could fill the chapter with names and stories—Ashkan Soltani, Raquel Romano, Chris Soghoian, others—but our needs are much greater than the prominent early adopters who made the leap from technical roles into the development of security policy. Technologists need to permeate policy at all levels, not just in the most visible roles. They need to be on legislative staffs, in regulatory agencies and nongovernment watchdog organizations, members of the press, and think tank policy wonks. We need a lot more of this than we have today.

There are programs to put technologists into policy positions. TechCongress is a fellowship program housed at New America, and it places technologists on congressional staffs. The Open Web Fellowship program places technologists within nonprofit organizations. Its focus is currently on organizations that work to protect the open Internet and more broadly to serve the public interest on issues of Internet policy.

Other programs try to harness technology for policy. Code for America is focused on plugging people with engineering and other technology skills into local governments to affect how systems are designed and implemented.

The Electronic Frontier Foundation, where I also serve on the board, has long blended technological and policy expertise. So does the Electronic Privacy Information Center, where I used to serve on the board. Through its Speech, Privacy, and Technology project, the ACLU focuses on the civil liberties impact of new technologies. Other organizations, like Human Rights Watch and Amnesty International, are beginning to tread into this area, albeit more slowly than I would like.

Many universities now offer interdisciplinary degree programs that blend technology and policy. MIT houses the Internet Policy Research Initiative, which offers courses that provide students with an integrated understanding of technology and public policy. Georgetown Law has the Center on Privacy and Technology. Many schools offer joint law and technology degrees. I teach at the Harvard Kennedy School of Government as part of its Digital HKS program.

These are great, but they're still all exceptions. We need to create a viable career path for public-interest technologists. We need courses and degree programs that blend technology and policy. We need internships, fellowships, and full-time jobs in organizations that need these skills. We need technology companies to offer sabbaticals for staff wanting to explore this path, and to value their experience in policy after they return to the business world. We need a career path that ensures that even though newcomers to this field won't earn as much as they would in a high-tech startup, they will have promising professional futures. The security of our computerized and networked society—meaning the security of ourselves, families, homes, businesses, and communities—depends on it.

A good model can be found in public-interest law. In the early 1970s, there was really no such thing. But after the Ford Foundation and other philanthropies decided to support fledgling public-interest law firms, the number of attorneys in the field exploded. In the late 1960s, there were 92 public-interest law centers in the US; by 2000, there were over a thousand. Today, 20% of the graduating class of Harvard Law School go directly into public-interest law, rather than starting at a law firm or a corporation. That experience is valued and serves these lawyers well in their careers, wherever they end up next.

Computer science isn't like that. Practically none of Harvard's graduating class, or that of any other university, go into public-interest technology. It's not a career path that programmers and engineers generally think about. I don't mean to blame the students here. There aren't public-interest jobs waiting for these people, nor does public-interest experience become an important part of their résumés.

This need to combine technology and policy transcends security. Nearly all of the major policy debates of the 21st century will involve technology. Whether the subject is weapons of mass destruction, robots, cli-

mate change, food safety, or drones, understanding policy demands understanding the relevant science and technology. If we don't get more technologists working on policy, we'll wind up with bad policy.

More generally, we need to start making moral and ethical and political decisions about how the Internet+ should work. We've built a world where programmers had an inherent right to code the world as they wanted to see it, indemnified against any harm they might have caused along the way. We accepted it because what they decided didn't matter very much. Now it very much matters, and I think this privilege needs to end.

You, the reader, can help bring this all about. We've been mesmerized by the incredible promise of these technologies, while failing to anticipate the problems. My hope is that the news stories of the past couple of years—and this book—have changed that. Now you have to push against the status quo. Encourage your elected officials to take these threats seriously. Make Internet+ security and privacy a campaign issue. It won't matter to our leaders if it doesn't matter to us.

The Internet+ is coming. With little forethought or architecting or planning, it's coming. It's going to change everything in ways we can only imagine and in ways we can't yet imagine. It'll change security, too: more autonomy, more real-world consequences, fewer off switches, and much greater risks.

It's coming faster than most of us think, and certainly too fast for us to prepare for with the tools we have now. We need to do better. We need to get ahead of it. We need to start making better choices. We need to start building security systems as robust as the threats. We need laws and policies that address the threats and the economics and the psychology properly, and won't become obsolete with changing technologies.

Our only hope of getting there is to bring together technologists and policy makers in that mythical *Star Trek* briefing room to work this out. Now.